A NIST BLUEPRINT FOR SECURING DIGITAL SUPPLY CHAINS_

INTRODUCTION_

Supply chain security has become one of the most important yet challenging issues facing organizations today. Advanced threat actors have sought to replicate the model of the SolarWinds attack by incorporating malicious code into seemingly valid products and updates long before they are delivered to the customer. Cross-cutting supply chain vulnerabilities such as Log4j and BootHole have caused widespread exposure for organizations and countless lost hours spent applying emergency patches. The Department of Homeland Security recently provided a detailed analysis of these types of risks in its 2022 document, Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry.

Collectively, these issues represent a new class of enterprise risk. Unlike typical risks that arise from inside the organization, such as an internal user clicking on a phishing email, supply chain risks are uniquely inherited from outside sources and embedded within the technology the organization relies on. Every piece of technology, from the highest-end server to the smallest IoT device, has a complex backstory involving dozens of suppliers and subsuppliers of software, hardware, and firmware components. Each step of this origin story is necessary for the delivery of complex equipment, but each step is also a chance for vulnerabilities, misconfigurations, or threats to be introduced into the final product. And put simply, organizations rarely have direct control – let alone visibility – into the process.

However, just because an organization doesn't directly control the supply chain doesn't mean it can't mitigate supply chain risks. A strong supply chain security program gives organizations the tools and processes needed to independently audit and verify that all their technology is genuine, unaltered, and free from vulnerabilities and threats. NIST's Special Publication SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, provides a practical blueprint for how this can be done at the enterprise level, whether in the private sector or in federal agencies. This document calls out the need for a broad, coordinated approach that covers the full lifecycle of technology and also includes all levels of an organization, from executive leaders to business/mission leaders and operational staff.

This document summarizes the key recommendations in SP 800-161 and shows how organizations can put those recommendations into practice using a Supply Chain Security platform. Specifically, readers will learn the following:

- An overview of Device Supply Chain Security and what makes it different from traditional cybersecurity
- A risk and impact-based analysis of supply chain attacks
- A practical guide to implementing SP 800-161 for infrastructure code, including:
    - How to implement a cross-functional approach to supply chain security and how to deliver the unique capabilities required for each job role
    - How to implement supply chain security across the lifecycle of information and communication technologies (ICT) from acquisition through end-of-life
    - How to use Software Build of Materials (SBOMs) to identify upstream supply chain risks
    - How to perform risk analysis of critical software running on devices such as laptops, servers, networking, and IOT
    - How to provide continuous integrity-checking and alerting of critical code on equipment and assets

We believe this information will help organizations develop a straightforward and successful approach to supply chain security that can adapt to changing demands while avoiding many of the most common pitfalls.

KEY REQUIREMENTS OF A SUPPLY CHAIN SECURITY STRATEGY_

Supply chain security is an incredibly broad discipline. Every technology asset has a supply chain – every physical piece of equipment, internal component, application, cloud service, open-source project, and so on. The impacts of these technologies are felt across an entire organization, from executives to business/mission managers to hands on IT and security staff. As such, it is important to recognize that supply chain security is bigger than an individual tool or feature, but instead requires a consistent, coordinated approach that involves all levels of an organization and spans the full lifecycle of a given asset.

SP 800-161 covers these issues in depth, both highlighting some of the fundamental challenges of supply chain security as well as the key capabilities organizations will need in order to address them. In this section, we will review these key challenges and requirements and show how organizations can begin to take action today.

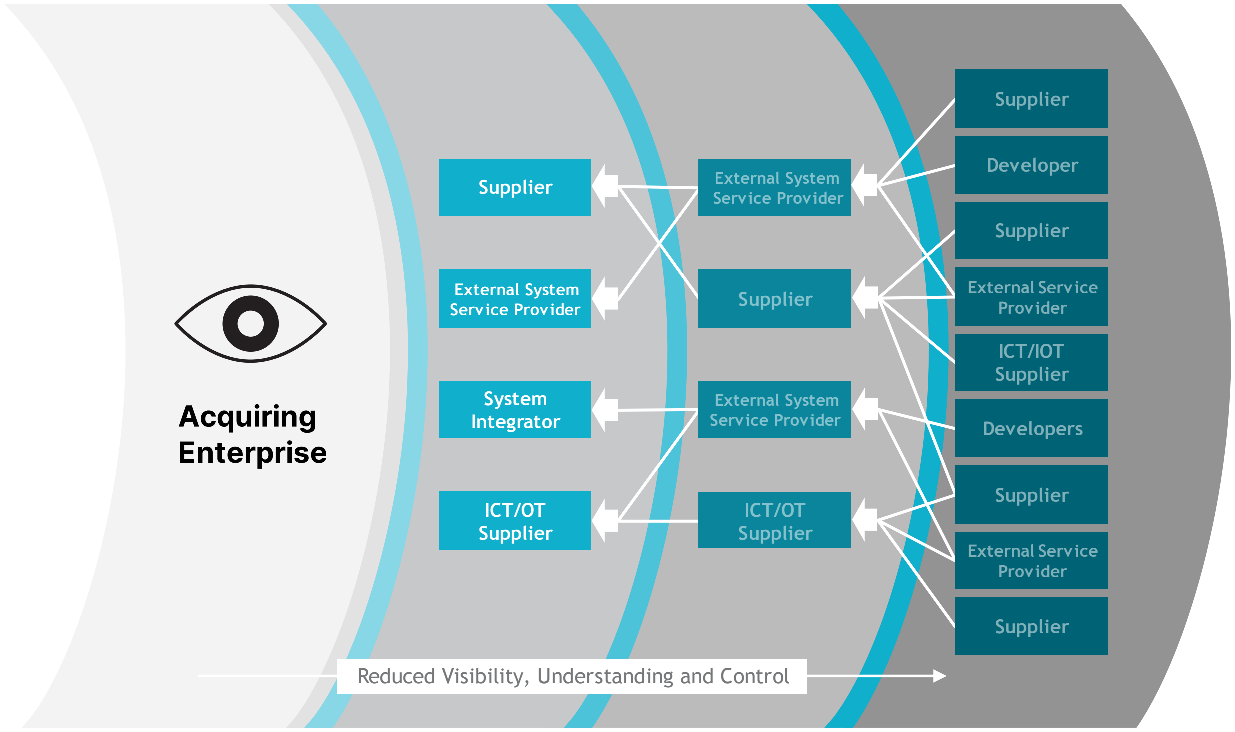
1 - Addressing Information Asymmetry

> *Identifying cybersecurity risks throughout the supply chain is complicated by the information asymmetry that exists between acquiring enterprises and their suppliers and service providers. Acquirers often lack visibility and understanding of how acquired technology is developed, integrated, and deployed and how the services that they acquire are delivered.*
>
> NIST SP 800-161

One of the biggest issues of the supply chain is that suppliers naturally know more about the products or elements that they produce than the buyer does. In most cases, this is a feature of the supply chain, not a bug. A company buying a laptop just wants an asset that works and doesn't need to know the minutiae of how to build a laptop. The same is true even for the laptop OEM, who doesn't need to know the low-level details of building SSD drives or USB-C adapters, and instead can farm that work out to other more focused suppliers who can achieve better functionality and costs. It is important to recognize that technology products and their supply chains are abstracted by design.

However, while this system is extremely efficient, it introduces serious problems when it comes to auditing the security and integrity of a final product. As more details are outsourced, visibility and control are increasingly eroded. As the NIST illustration below shows, each layer in the supply chain lacks visibility into its upstream suppliers, and the effect compounds over multiple steps. This makes it easy for vulnerabilities or even malicious threats to be introduced into products without the customer recognizing the problem.

AN ENTERPRISE'S VISIBILITY, UNDERSTANDING, AND CONTROL OF ITS SUPPLY CHAIN


Acquiring Enterprise
Supplier
External System Service Provider
System Integrator
ICT/OT Supplier
External System Service Provider
Supplier
External System Service Provider
ICT/OT Supplier
Supplier
Developer
Supplier
External Service Provider
ICT/IOT Supplier
Developers
Supplier
External Service Provider
Supplier
Reduced Visibility, Understanding and Control

Source: NIST SP 800-161

– Putting Supply Chain Security Into Practice –

While the risks of a complex supply chain are clear, it is not reasonable to expect that every enterprise can become an expert on every layer of its supply chain. An IT Procurement team doesn't have the time or resources to investigate how the firmware within a PCIe controller or the dozens of other critical components should behave. Likewise, if a developer had to do a line-by-line security review of every open-source package, it would quickly defeat the purpose of using readily available open-source projects in the first place.

However, this is where supply chain security tools can fill the gap. These tools have the necessary industry and domain expertise to automatically unravel the complexities of the supply chain and assess all relevant hardware, firmware, and software in order to identify problems. Simple scans should allow organizations to audit even the most complex products and systems to pinpoint issues, even if they occur deep in the supply chain. Key steps can include the following:

1. **Validate Software Bills of Materials (SBOMs)** - Organizations increasingly require their suppliers to provide detailed SBOMs to clearly enumerate the critical code within their products. This is a critical first step in addressing information asymmetry because it says what should be in a product. The challenge is that many organizations are not equipped to validate that what the SBOM says is accurate. While it is trivial to verify the OS version of a device, it can be far more challenging to verify the dozens of different types of low-level code and firmware within a given asset. A supply chain security platform can provide simple audits of these many types of code to verify that the actual products and updates align with the official vendor-supplied SBOMs.

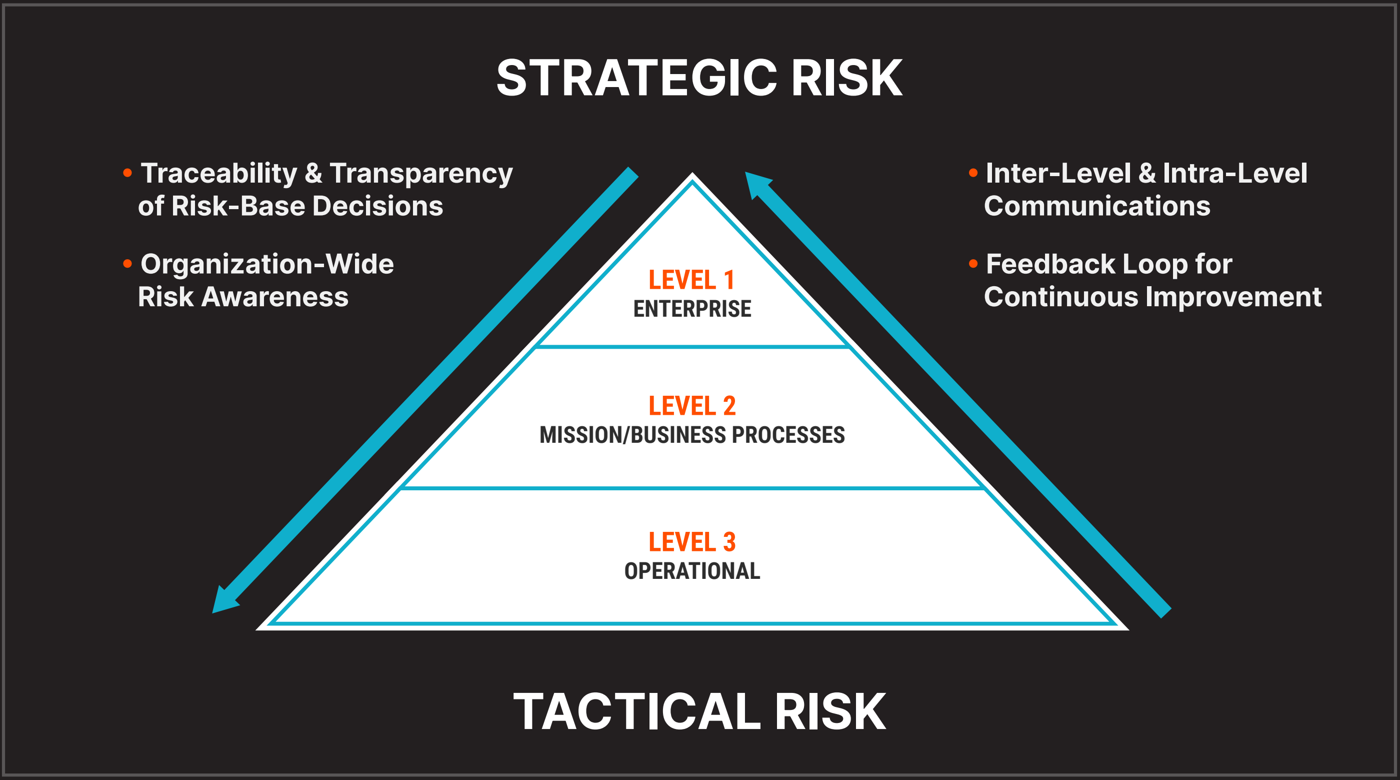
2. **Identify Vulnerabilities and Misconfigurations** - Of course, just because an asset is running the "correct" code, that doesn't mean that the code is secure. Organizations must be able to analyze the many types of critical code (software, OS, firmware, etc.) within an asset to find vulnerabilities, particularly any critical vulnerabilities or vulnerabilities being exploited in real-world attacks. Low-level device configurations pose another key area of information asymmetry. Even a basic laptop relies on a suite of low-level protections that protect the boot integrity of the device. These protections require fine-grained coordination between the chip vendors, OS vendors, and OEMs. Even a small oversight can render the most modern systems exposed to attack. Supply chain security tools can analyze that all available protection mechanisms are properly configured and working as they should.

3. **Assess Assets for Threats** - Attackers try to take advantage of information asymmetry in the supply chain by embedding threats within code that is presumed to be "good." Such attacks can target any level of code and all phases of a product lifecycle, including product updates. Supply chain security tools provide unique capabilities to identify these threats. First, these tools can verify that all code matches "known valid" provided by all the relevant suppliers. This ensures that an asset hasn't been tampered with or altered while in the supply chain. Next, tools can analyze assets for both known and unknown low-level threats. This could include looking for indicators of implants, backdoors, and rootkits while also analyzing the behavior of all critical assets to identify new threats that have not previously been seen in the wild.

2 - Implementing Supply Chain Security Across the Organization

SP 800-161 heavily emphasizes one key concept: supply chain security is an organizational challenge that requires coordinated effort and support across multiple groups. The document builds upon the three-tiered approach to risk management defined in NIST's SP 800-39 on Managing Information Security Risk. This approach defines roles and responsibilities in the following levels as shown in the figure below:

MULTILEVEL ENTERPRISE-WIDE RISK MANAGEMENT


STRATEGIC RISK
• Traceability & Transparency of Risk-Base Decisions
• Organization-Wide Risk Awareness
• Inter-Level & Intra-Level Communications
• Feedback Loop for Continuous Improvement
LEVEL 1
ENTERPRISE
LEVEL 2
MISSION/BUSINESS PROCESSES
LEVEL 3
OPERATIONAL
TACTICAL RISK

Source: NIST SP 800-161

1. **Enterprise (Level 1)** - Level 1 includes executive leadership roles including the CEO, CIO, CISO, and others to define and support the overall supply chain security strategy. This level defines the strategic goals of the program and the organization's high-level tolerance for risk.

2. **Mission and Business Processes (Level 2)** - Level 2 must assess supply chain security in terms of the business or mission. Level 2 can include business line managers, program and project managers, engineering, R&D teams, and many others. Level 2 will often rely on the technical expertise and recommendations from Level 3 operational staff and also be able to report key metrics and information up to Level 1 staff.

3. **Operational (Level 3)** - Level 3 focuses on the specific risks to the organization's systems and services. This can involve procurement teams as well as the IT staff that directly owns and operates those systems and services. This level can also include information and cybersecurity experts with detailed insight into current threats, including threat indicators and adversary tactics being employed in the wild. Level 3 staff will provide the most detailed recommendations and reporting that will ultimately be used by the higher levels.

– Putting Supply Chain Security Into Practice –

SP 800-161 calls out that supply chain risks are organizational risks, and mitigating them demands an organization-wide effort. This includes not only tasks within each level but also clear communication and coordination between teams and levels. For example, executive staff won't be able to establish an effective strategy without insight into how the supply chain affects business units. Those business leaders, likewise, won't be able to accurately assess their risks without the technical risks to their assets and how they are targeted by real-world adversaries. As such, it is essential for organizations to not only develop multi level strategies but also to establish a sort of supply chain *lingua franca* that allows different teams to consistently and accurately communicate information about supply chain risks and drive well-informed actions.

As such, let's look at the way that people, processes, and tools can be applied at each of the levels defined by SP 800-161:

1. **Enterprise (Level 1)** - Level 1 leaders will define the overall strategy of the program and ultimately hold the teams in Levels 2 and 3 accountable. First and foremost, executive leaders must commit to making supply chain security a priority. Key tasks can include:

    a. Establish a strong executive leadership team and define the governance structures for the overall program.

    b. Engage with the various business units and mission stakeholders to better understand the risks that the supply chain poses to various aspects of the organization. Leaders may also want to engage with legal and compliance teams to understand the potential legal and financial impacts of a supply chain compromise.

    c. Define and communicate organizational priorities and risk tolerance that Level 2 and 3 teams can use to develop more tactical policies.

    d. Define the key metrics for various business units in order to measure the success of the program.

2. **Mission and Business Processes (Level 2)** - Level 2 teams must be able to assess, monitor, and respond to risks in the context of the actual business functions or the agency mission. This requires teams to specifically define how various technologies and services are used to support key business or mission goals, the potential impact of a supply chain threat or disruption, and the likelihood of such an event occurring.

a. Perform a full assessment of the technology, people, and processes that support the business or mission. For example, a specific business function may rely on software developed internally or by 3rd party vendors. That code may run on locally or cloud-hosted servers, and those systems likewise may rely on enterprise network infrastructure. A disruption or compromise to any of these components could have serious consequences to the overall mission.

b. Engage with security teams and other Level 3 staff to better understand the current threat landscape. The goal is to understand both the potential impact and likelihood of supply chain events based on events and threats in the wild.

c. Develop specific policies and requirements to align with the business or mission. This can include engaging with suppliers, developers, service providers, or any entity that contributes to the business unit. This can include requiring vendors to supply detailed SBOMs, adhere to secure development practices, and assess all code from their suppliers and sub-suppliers.

d. Establish measures to assess and verify that all aspects of the supply chain are conforming to established policies. This will likely require supply chain-specific tools and/or additional engagement with Level 3 operational staff.

e. Develop systems or processes to monitor key supply chain metrics. These will need to include tangible security metrics such as vulnerabilities prioritized by criticality, threats, time to resolve, etc.

3. **Operational (Level 3)** - Much of the technical work will fall to the operational staff in Level 3. This can include IT staff, procurement teams, cybersecurity teams, QA engineers, or any staff that has direct responsibility for the ways that technology is procured, operated, or maintained.

a. Establish deep technical and industry insight into the equipment and assets that they support. For example, a Level 3 team responsible for buying and/or maintaining critical servers must be aware of the many device-level vulnerabilities that can affect servers and then be able to evaluate and audit any acquired servers for potential problems. Supply chain security tools can be highly valuable for providing this level of insight.

b. Establish and maintain supply chain-specific threat intelligence. This can include systems to quickly identify and prioritize new supply chain level vulnerabilities, revoked or vulnerable bootloaders, drivers, and more. Staff will also need intelligence involving active threat campaigns in the wild. These real-world insights into threat trends will be critical in order to properly shape the strategy defined by Level 1 and Level 2 teams.

c. Develop tooling and processes to easily and regularly audit supply chain assets. This should include newly acquired assets as well as all updates in order to verify the integrity of the asset and to detect any known or unknown threats.

d. Establish response playbooks or processes to quickly respond to newly detected threats or vulnerabilities.

e. Establish methods to collect and report key metrics for both Level 2 and Level 1 teams.

Finding and mitigating vulnerabilities and threats in the supply chain can be a highly technical and time-consuming task that requires a variety of specialized skills and capabilities. As such, this is one of the key areas in which supply chain security tools can be invaluable. Instead of requiring teams to become experts in hardware manufacturing, firmware, boot processes, and low-level software, staff must be able to quickly scan an asset in order to verify that it is authentic, unaltered, and free from vulnerabilities and threats. An organization will also likely want to standardize on a set of supply chain security tools that can be used across multiple operational teams. This can ensure that the organization maintains consistent visibility and context throughout the lifecycle of an asset and has a consistent way of reporting information up to higher levels in the organization.

3 - Implementing Supply Chain Security Across the Technology Lifecycle

Supply chain security also extends across the full lifecycle of an asset from the earliest phases of the selection process through end-of-life. It is worth noting that many of the most recent supply chain attacks, such as the SolarWinds attack, were introduced via product updates to solutions that were already deployed. Let's look at some of the key steps teams should take at various phases of the technology lifecycle.

– Putting Supply Chain Security Into Practice –

Procurement

Procurement teams naturally play one of the most critical roles in the supply chain security strategy as they directly interact with supply chain partners. These teams will require a variety of skills as they will need to define business relationships and set expectations with vendors while also having the technical expertise to independently evaluate prospective technologies. Key steps will include:

1. **Define security requirements in selection criteria** - Cost/functionality issues often dominate technology selection criteria, so it is important for procurement teams to clearly define security requirements as part of the decision-making process.

2. **Define expectations of vendors and suppliers** - As part of the business relationship, teams will need to define what is expected of prospective vendors in terms of security. This may include

    a. The need to provide detailed SBOMs of all critical code, even at the firmware and microcode levels

    b. Define the need for secure coding practices

    c. Define the need for secure updating mechanisms

    d. Define restrictions on suppliers or regions that the vendor does business with

    e. Define the need to notify of any changes in suppliers or product SBOMs

3. **Independently vet prospective products** - While it is important to define what vendors should do, it is equally important that teams can independently verify that any products and services actually meet those expectations, including

    a. Verify evaluated products actually match the vendor-supplied SBOM

    b. Scan all critical software, firmware, and components for known vulnerabilities

    c. Perform product-level assessments to ensure all protections are prosperity enabled

    d. Evaluate update mechanisms for all critical code to ensure mechanisms are both secure and that updates are regularly provided

Receiving and Initial Deployment

Once a technology is selected, organizations will need to put those assets into service. This process can continue repeatedly over months and years as the organization buys and deploys additional assets. Additionally, individual assets may pass through several entities during the course of fulfillment such as product resellers, warehousing, and delivery logistics. As such, teams must be ready to verify that the actual product that is received meets all expectations in terms of security, including:

1. **Verify product integrity** - Staff should verify that each asset that is received conforms to the vendor-supplied SBOM. Additionally, staff should cryptographically match all critical code to the known, valid code supplied by the vendor or relevant supplier or sub-supplier.

2. **Assess for vulnerabilities and threats** - Staff should scan each asset for the presence of vulnerabilities or threats such as implants and other malicious code. This is a critical step since new vulnerabilities and threats are discovered on a regular basis. A product that had no known vulnerabilities when it was selected could easily have vulnerabilities that were discovered weeks, years, or months later and are being actively exploited in the wild.

3. **Establish a process to support remote users and sites** - Organizations are increasingly distributed with employees either working remotely or in offices that lack extensive IT support. If assets need to be directly shipped to these locations, IT teams should include the ability to remotely scan these assets as part of the initial system setup.

Continuous Monitoring and Response

Supply chain security doesn’t stop once an asset is deployed. Virtually all technology requires regular vendor updates which can introduce new vulnerabilities and threats. Supply chain threats are some of the most difficult threats to detect since they often arrive in the guise of “good” or approved code and can even subvert the operating system itself in order to hide or evade security controls. Key steps include:

1. **Regular vulnerability scanning** - Teams will need to regularly scan all critical code for vulnerabilities. These efforts often require additional measures beyond traditional vulnerability scans, which often focus on application and OS-level vulnerabilities. Teams will need to ensure the ability to scan down the firmware, bootloaders, and other low-level code below the operating system. Teams will also need to scan critical assets, such as networking infrastructure which are often not covered by regular vulnerability scans.

2. **Continuous threat detection** - Teams will need to look for the presence of supply chain threats on a regular basis. This could include the presence of malicious code embedded within products or software updates as well as low-level implants, backdoors, and rootkits embedded within system or component firmware.

3. **Behavioral monitoring** - Some of the most devastating supply chain attacks have stemmed from vendors who have been compromised by either an internal or external threat actor. In these cases, malicious code will arrive as properly signed and seemingly valid code from the vendor. In these cases, it is critical that teams have the ability to monitor the behavior of critical code as well as updates in order to identify malicious or suspicious behaviors.

4. **Threat intelligence monitoring and sharing** - The threat landscape is always evolving, and teams must stay abreast of the latest developments. Teams should establish reliable processes and feeds for obtaining information on new threats and vulnerabilities. These updates should also be shared with business and executive leaders in order to properly update organizational security policies and priorities.

5. **Alerting and response** - Teams will naturally need to ensure that any problems can be quickly contained and mitigated. This may include the need for automated alerting and response workflows and playbooks based on the identified risk.

NIST CONTROLS_

SP 800-161 also provides a list of specific security controls that can be applied to a supply chain security program. These controls are sourced from SP 800-53, which establishes the definitive list of security controls that are referenced across many industry and security frameworks. For insight into how this document has evolved to reflect the increasing use of device-level software and firmware, readers can review the Eclypsium paper Firmware, Supply Chain, and Frameworks: NIST SP 800-53 (PDF).

However, we have also included a summary list of controls that are called out in the SP 800-161 document and specifically those that can be addressed using a supply chain security platform such as Eclypsium.

Assessment, Authorization, and Monitoring	
CA-2 Control Assessments	The required skills include general knowledge of risk management concepts and approaches as well as comprehensive knowledge of and experience with the hardware, software, and firmware system components implemented.
CA-7 Continuous Monitoring	The terms “continuous” and “ongoing” imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Automation supports more frequent updates to hardware, software, and firmware inventories, authorization packages, and other system information.
Configuration Management	
CM-2 Baseline Configuration	Automated mechanisms that help organizations maintain consistent baseline configurations for systems include configuration management tools, hardware, software, firmware inventory tools, and network management tools. Retaining previous versions of baseline configurations to support rollback include hardware, software, firmware, configuration files, configuration records, and associated documentation.
CM-6 Configuration Settings	Identify, document, and approve any deviations from established configuration settings
CM-7 Least Functionality	Code execution in protected environments applies to all sources of binary or machine-executable code, including commercial software and firmware and open-source software.
CM-8 System Component Inventory	System components are discrete, identifiable information technology assets that include hardware, software, and firmware. Detect the presence of unauthorized hardware, software, and firmware components within the system...
CM-14 Signed Components	Prevent the installation of software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
Contingency Planning	
CP-9 System Backup	Security-related information includes inventories of system hardware, software, and firmware components.

Identification and Authentication

IA-5 Authenticator Management	(a) For public key-based authentication: (1) Enforce authorized access to the corresponding private key

Incident Response

IR-4 Incident Handling	Analyze malicious code and/or other residual artifacts remaining in the system after the incident. Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.

Maintenance

MA-3 Maintenance Tools	Approve, control, and monitor the use of system maintenance tools; Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel on media, cloud-based, or downloaded from a website.

Risk Assessment

RA-3 Risk Assessment	Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm... Assess supply chain risks associated with organization-defined systems, system components, and system services and Update the supply chain risk assessment when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.
RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications Enumerating platforms, software flaws, and improper configurations; Measuring vulnerability impact; Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-9 Criticality Analysis	The functional decomposition includes the identification of organizational missions supported by the system, decomposition into the specific functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions, including when the functions are shared by many components within and external to the system.

RA-10 Threat Hunting	Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls;
System and Services Acquisition	
SA-3 System Development Lifecycle	Acquire, develop, and manage the system using organization-defined system development life cycle Technology refresh planning may encompass hardware, software, firmware, processes, personnel skill sets, suppliers, service providers, and facilities.
SA-8 Security and Privacy Engineering Principles	Organizations can apply systems security and privacy engineering principles to new systems under development or to systems undergoing upgrades...given the current state of hardware, software, and firmware components within those systems.
SA-10 Developer Configuration Management	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components. The integrity checking mechanisms can also address counterfeiting of software and firmware components. Organizations verify the integrity of software and firmware components, for example, through secure one-way hashes provided by developers. Delivered software and firmware components also include any updates to such components.
SA-11 Developer Testing and Evaluation	Require the developer of the system, system component, or system service to perform attack surface reviews. Attack surfaces include any accessible areas where weaknesses or deficiencies in the hardware, software, and firmware components provide opportunities for adversaries to exploit vulnerabilities.
SA-17 Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce...a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects. Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.
SA-20 Custom Development of Critical Components	Reimplementation or custom development of such components may satisfy requirements for higher assurance and is carried out by initiating changes to system components (including hardware, software, and firmware) such that the standard attacks by adversaries are less likely to succeed.

SA-22 Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer Discussion: Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts.
System and Communication Function	
SC-37 Out of Band Channels	Out-of-band channels include local, non-network accesses to systems; network paths physically separate from network paths used for operational traffic;
System and Information Integrity	
SI-2 Flaw Remediation	Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation. The need to remediate system flaws applies to all types of software and firmware.
SI-3 Malicious Code Protection	Malicious code protection mechanisms include both signature- and nonsignature-based technologies.
SI-4 System Monitoring	System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at external interfaces to the system. Internal monitoring includes the observation of events occurring within the system.
SI-7 Software, Firmware, and Information Integrity	Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: Firmware interfaces include Unified Extensible Firmware Interface (UEFI) and Basic Input/Output System (BIOS). Perform an integrity check of software, firmware, and information] (one or more): at startup; at transitional states or security-relevant events or organization-defined frequency. Security-relevant events include the identification of new threats to which organizational systems are susceptible and the installation of new hardware, software, or firmware. Transitional states include system startup, restart, shutdown, and abort. Employ automated tools that provide notification to organization-defined personnel upon discovering discrepancies during integrity verification. Employ centrally managed integrity verification tools. Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information. Verify the integrity of the boot process of organization-defined system components. Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation

Supply Chain Risk Management	
SR-2 Supply Chain Risk Management Plan	Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;
SR-3 Supply Chain Controls and Processes	Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.
SR-4 Provenance	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements.
SR-6 Supplier Assessment and Review	Employ (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes
SR-11 Component Authenticity	Train organization-defined personnel to detect counterfeit system components (including hardware, software, and firmware).

CONCLUSIONS AND NEXT STEPS_

The complexity and criticality of digital supply chains impacts every modern organization, whether federal or commercial. The supply chain for digital devices, specifically, impacts them whether they are "cloud-first" in outlook or are dependent on internal devices for their knowledge workers, systems and processes.

The purpose of NIST's Special Publication 800-161 is to "provide guidance to enterprises on how to **identify**, **assess**, **select**, and **implement risk management processes and mitigating controls across the enterprise** to help manage cybersecurity risks throughout the supply chain." If your organization needs assistance identifying, managing and mitigating the risks embedded in the device-level code, firmware and microcode that exists throughout your supply chain, visit www.eclypsium.com or call +1 (833) FIRMSEC.